

CONTENTS

HUGO CORNWALL INTERVIEW	4
COSMOS GUIDE	6
TELECOM INFORMER	8
NASTY BUSINESS	10
LETTERS	12
NEW DEVELOPMENTS	18
2600 MARKETPLACE	19
PHONE NEWS	20

2600 Magazine
PO Box 752
Middle Island, NY 11953 U.S.A.

SAVE YOUR ADDRESS LABEL FOR LOGIN
TO THE NEW PRIVATE SECTOR BULLETIN BOARD!
(201) 366-4431

26000



Volume 4, Number 2

February, 1987

\$2

The Monthly Journal of the American Hacker



2600 WANTS YOU!

Join the staff of 2600. It is simple. Just compile any information you have so it is easily understandable and send it to us. We accept hardcopy and usboards. We will also accept information on floopies—call us if you wish to do that.

- ◆ We need:
- ◆ Profiles of long distance companies
- ◆ Profiles of computer systems
- ◆ Reviews of popular security devices
- ◆ Lists of interesting phone numbers
- ◆ Lists of interesting reference books and magazines
- ◆ Updated materials on using things like AIDS, CNA
- ◆ Interesting true stories
- ◆ Data that can be a good reference
- ◆ Maps of computer networks
- ◆ Analysis of new legislation

We would like:

- Legitimate access to various computer networks
- You to continue to send your comments and questions
- You to continue to send clippings from local papers and magazines
- You to help keep us informed

Things we could always use:

- * Printers, computers, telephones, and interesting devices
- * More modernized office equipment
- * A 2400 baud modem

If you send us articles or data, please request a by-line otherwise we will not print one.

If you send us hardware, please make sure it is not stolen. We do not want your troubles.

We pay our writers a small amount. Perhaps that will be the incentive you need. We also pay people who get advertsing for us. Call us for more details.

All contributors, please send your gifts to: 2600, P.O. Box 99, Middle Island, NY 11953-0099, or call 51673-12600.

We've been swamped with mail from people who either wanted to come at the old rule or who wanted to comment on our new style. Please forgive us if we seem to take a little longer to process your particular request—this article's for outweighed our wildest dreams.

This probably means we're doing quite well, but it's always hard to be conclusive. Our experiments with several newstands across the country appears to be succeeding as well, and we hope to have a distributor before long. Before long, 2600 will be a household word. Look for a list of newstands we can be found at in a future issue.

This month we're happy to present an exclusive interview with one of Britain's most notorious hackers, Hugo Cornwall. It's one of many we'll be presenting and we think there's a lot to be learned from

this observations.

We've also got an article on COSMOS that many readers will no doubt fail to understand entirely. This has always been a problem for us here as we must constantly try to please both the beginners and the advanced hackers among us. One thing we believe everyone can get out of this article is a refutation of all of the different ways your phone service can be categorized and how easy it is to change this with a simple stroke of the keyboard. It might lend some insight as to why you didn't get what you asked for or perhaps how you managed to wind up with a prison phone line.

Phones and computers are incredible and the two together can be quite scary. The purpose of our magazine is to show you what's going on with both—in as many ways as possible.

STAFFBOX

Editor and Publisher
Twenty Six Hundred

Associate Editors

Eric Corley David Ruderman

Office Manager

Helen Vicary

PSOS Operations

Tom Allich

Writers: John Drake, Paul Esley, Dan Foley, Mr. French, Emmanuel Goldstein, Chester Holmes, The Kid & Company, Lex Luther, Bill from FINOC, Mike Salerno, The Shadow, Silent Switchman, and the usual anonymous bunch.

Artists: Dan Holder, Mike Marshall, Tish Walter Koch

2600 (ISSN 0720-4551) is published monthly by 2600 Enterprises, Inc., 7 Stewart Lane, Syosset, NY 11791. Second class postage printed pending at Syracuse, New York.

POSTMASTER: Send address changes to 2600, P.O. Box 752, Middle Island, NY 11953-0075.

Yearly subscription: U.S. and Canada: \$15 individual; \$40 corporate; Overseas: \$25 individual; \$55 corporate.

AN INTERVIEW WITH HUGO

By John Deeks

Where did you get your ideas from?
It was actually derived over a rather drunken lunch with the publisher, all that I had decided that it was to be a pseudonym, but I will explain genesis. Originally I was going to be Hugo Cornwall with an "E" rather than an "A" because Bruce Cornwall is the real name of John LeCarre, a spy writer who I rather admire—hence also got a number of talented brothers and sisters. So the original thought was that it was going to be, in order to mislead the public, yet another member of a very talented family.

But at the time a number of the Elite hackers were operating under the name Persuase, a SIG called Persuase which had originally been called The Prizes of Persuase for fairly obvious reasons. So Persuase is in Cornwall so that it flows I guess about. So we decided to call it Cornwall with an "A" and Hugo was chosen as a Christian name simply because I think it is one of the less likely names I could possibly have.

How did you start off as a hacker?
Not very deliberately. I got into communicating computers probably very early round about '78 and I just got very curious about what was going on in big computers and how to do it in and searching and so one particularly interesting thing that I never thought of it particularly as naughty or illegal but if I picked up a phone number or a password that I simply carried on collecting it. I ended up with a few sheets full of these things and I would pass them around to friends out of curiosity and it wasn't probably until '82 or '83 that I became aware that there were not just other people collecting [in a] similar sort of way but there was a proper culture outlet called Hacking and I said, "OK, well I suppose I am a hacker."

What did you do previous to hacking—did you have any other interests that were along the same line?
I guess I have been interested in what I call in the book the larger area of both phreaking. In other words, making technology misbehave in the most possible way. I got interested in that when I was an undergraduate at Oxford and everyone I knew was interested in phone phreaking and that in fact one of the best phone phreakers was one of the dons and in the primitive sort of phone system that operated there you could really do a lot. So I was interested in that.

I certainly got interested in what we over here in England called bunker hunting. In other words, trying to find out secret sites used by the government and also by the U.S. government. There was, partly a political motive in that but it was really rather a lot of fun.

I got interested also in the brief illegal children band seen thing that was going on in this country. I got a radio amateur license and I got also very interested in

these parts of the radio spectrum that are not terribly well secured. In most countries in the world western world, you can buy books that tell you where all the various services lie. You can't in this country or you couldn't until very recently and I say [if] we were going to try to work out the pattern of the allocation of the frequency bands and then using radio scanners [to] actually eavesdrop on them. You know, although some of the stuff is now more widely known, there is a lot of the stuff that isn't known. There are a handful of people in this country who are really rather good at it.

How do the laws in the U.K. versus the U.S. encourage this type of investigation?
How do they encourage it? Well they discourage it really. It is done in two ways. First of all there is a lot less published in this country. We have got much tougher about what we publish. We don't have a Freedom of Information Act. Anything that is generated by the government is deemed to be secret unless [it] has been specifically released for publication so there is a lot of a lot less information that is openly available. So there is that one aspect. The other aspect is that a lot of our laws are all enveloping in theory though they're widely ignored in practice. There is a contrast to the United States in particular. I know less about Canada and that is if you look specifically at hacking there is no specific anti-hacking legislation. You can be done for stealing telephone time if you look at telephone hacking, stealing electricity sometimes. You can be done for stealing CPU time on a computer and recently they have done people for forging which is basically using passwords to which they are not entitled and that case is going to appeal.

What was your motivation for writing "The Hacker's Handbook"?
The motivation was that I was asked to do it and it was very very easy. The wife at the time was a man who was a bookie by interest and a publisher by profession writes/reads a note on a bulletin board saying does anyone want to write a book on hacking and I wrote back not very seriously. In effect saying [you] cannot be serious. It can't be done. He wrote back, said I don't know, call me back and we will have a chat about it. I rang up, said I'll do all the obvious things, why all the obvious things should be included and he sort of had a debate with me and at the end of it I said maybe it could be done. I wrote then a synopsis within 24 hours. 24 hours afterwards he said it was terrific, would I mind waiting two or three days till he had his editorial meeting, but he wanted to do the book and at the end of all that, you know, with me the book, beginning of the week I hadn't thought of writing the book. I hadn't thought of writing my book either and at the end of the week I actually had a contract.

So I would have never written a synopsis for the

book. I would have never finished it if not for that. But since there was the opportunity and I had a very rough thought about the synopsis, I thought, well, why not get it out. If there was a great burning desire, there was an opportunity, and I went to bed and wrote it. What has been the public response to the book since you wrote it?
There was a great deal of interest. The book was in several weeks on the Sunday Times Best Seller List so it was competing with some pretty popular titles. I think it got popular interest largely because of an interview on the Sunday Times rang up the head of the Carnegie Security Squad at Scotland Yard [and] asked the interview. The man had to read the book but said sufficient for her to be able to lead me a story. "The Condemned Hacker Book". This immediately made the book appear very very important and very very serious and after that book or a little bit more and after that my understanding the whole thing with a great degree of misapprehension.

These people who knew anything about hacking do not find it was not a very interesting book and I never thought that it would do that. It obviously excited a lot of other interest. I think people created the book for themselves—they badly wanted a book about hacking, they wanted to make hackers and some sort of hoodlum myth and my book happened to be accurate capture all of that interest. Though there was a great deal of lack in it.

One of the effects of the Scotland Yard condemnation is that the books that hadn't been very widely distributed up till then, the original print run was very small. It disappeared very rapidly from the bookshops and it created a further myth that the book had been banned in some way so everyone was rushing around the shop to get hold of them until about a few weeks when the book came out and received copies were free, people grabbed it like crazy for fear that it [was] really going to disappear.

About two weeks after the book was published, a couple of guys were arrested for hacking the British position and the newspaper reporters decided that one of these people was me, so there were headlines saying "Hacker Author Arrested" and things like that and again it really was that it all helped sales.

It was really quite a phenomenon and I do say to all hackers the situation that the book got was somewhat understood and I feel a little bit sorry about getting some hackers in sort of getting lucky.

In the first book you read a sponsorship for the Stars for the award, it wasn't there. What was Britain Telecom's response to the book and how did it influence you in a sequel?
Well, the decision to take it out wasn't mine. It was the publishers. I had it sent in three stages. I wrote in the

CORNWALL

a British hacker/author

first edition the sponsors was more compatible with values for the various companies and they gradually something disappeared. I don't know that British Telecom did anything very much other than to correct [the book] and what the publishers reacted not necessarily that things were getting a little bit hot and they [anticipate] trouble and removed the stuff so that they could show that they were being reasonable. I think that is the way it happened. British Telecom said that they didn't approve of that sort of thing, but you know there are hackers or British Telecom's staff as you might expect so you know I think to answer to my certain knowledge a lot of people within the telecom world at least get the idea the reason to believe that some of the British Telecom Security people were not impressed about the book because it made everyone a bit more alert about the use of passwords.

There is one other point also to show that a few of the books were actually sold either to computer security people or sold by them to, if you like, their customers in essence to say, "Look how easy it all is, read the book and be aware."

How would you say that U.K. Hackers would be different from U.S. hackers?
I think that the difference is of subtle rather than of essence. I think there are two areas of difference. First of all my guess is that the majority of U.K. people, U.K. computer enthusiasts, that have modern probably acquired them about two or three years after the majority of U.S. equivalents.

That's really a question of how modern are some. When I first got interested in computers, the only resources that were available were from British Telecom. You couldn't buy them on retail and they were very expensive. If you had them, you either had fully fledged ones, ones that had been modified for U.S. use and that was only of limited use or you had these very expensive ones which were no steered with British Telecom.

So you got this two or three year gap. The second way I think is that again although it wasn't the case for the most British enthusiasts, their first desktop they called into was going to be Prestel which is a videotex system. 75/1200 baud. The computer which is a video terminal that they had was for that reason. It meant that a lot of their hacking was either into Prestel or into systems which looked like it. Of course there was the university situation in the states where people would tend to be looking at mutual rate de grass telephone services 500/3000. I suppose that American hackers would call into The Source or into a BBS. My Prestel had been going for a bit then in the early eighties you started to get the BBS which people used 500/3000. I

(continued on page 111)

the telecom informer BY DAN FOLEY

Cellular Phreaking

The future hinted in the December issue of 2609 is already here. Cellular fraud is becoming a concern of the CPCCs (Cellular Phone Companies). Much fraud is from the same old source—the theft of cellular phones or even the entire car, resulting with the new “owner” making calls on the victim’s cellular ID (and phone bill).

Another form of fraud is from roamers (cellular users using their phones in a different city from where they signed up) who don’t bother to let the CPCC in the new city know their billing info.

Roaming will become more prevalent as more people buy cellular phones and use them while they travel. However this form of fraud will soon become a thing of the past, as the CPCC’s are creating a national billing data clearinghouse which will ensure that bills will reach the right user. This clearinghouse will also (further in the future) allow someone to call a cellular telephone, and the call will be correctly routed to wherever in the United States the phone happens to be.

Of more interest to the readers of 2609 is something that is quickly growing and represents the most dangerous threat to CPCC’s billing. Spoofing another cellular user’s ID isn’t as hard as it seemed.

Some of the more exotic schemes involve sending cellular IDs off of the airwaves as calls are being placed. Most CPCC’s don’t even bother to encrypt the ID signals (and you don’t even need to decrypt if the encryption algorithm doesn’t include time and date stamping). But there is even a simpler method than using an “ether” box (so called because the box snatches IDs out of the “ether”).

The easiest method by far needs the complicity of a cellular phone repair or installation shop. For many brands of phone the cellular ID is not in a ROM like “they” tell you, but instead is programmable. Motorola, for one, is supposed to have easy-to-follow

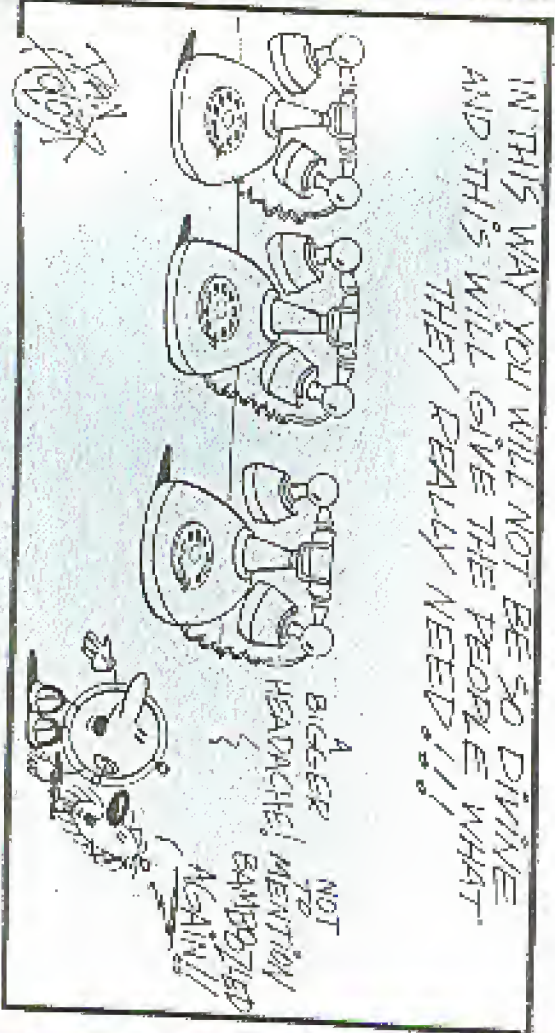
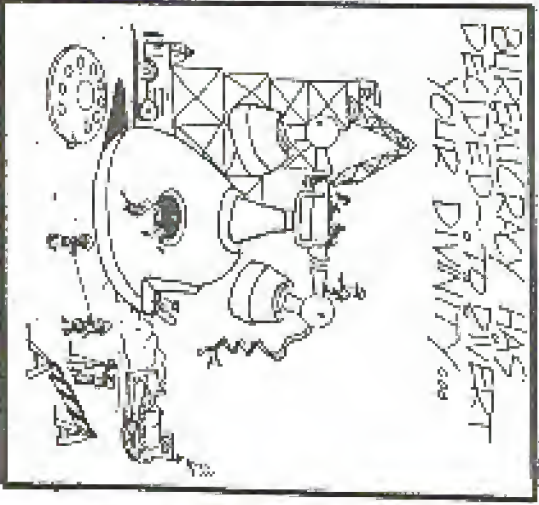
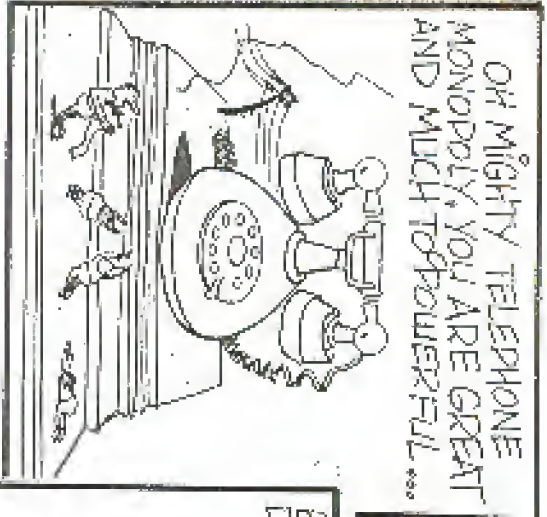
instructions in programming their phone’s cellular ID’s inside the repair manual. And even if the ID is recorded in a ROM, you can just burn a copy. Rumor has it that cellular ROMs are already available on the black market. Perfect for your local terrorist in cell in death threats and be untraceable, as the authentic would accuse the wrong person.

The Largest Cellular Companies

The largest cellular system in the world encompasses almost the entire Gulf of Mexico. On July 15 (coastal) (sic) Communications began serving from Brownsville, Texas in Mobile, Alabama, with a stretching office in Lafayette, Louisiana, and cell sites on offshore platforms out to about 100 miles from the coast. Coastal plans to target the oil business, fishing and other commercial marine operations. Airfare averages \$1.00 a minute, rather expensive, but they do provide a specialized service: Cellular rates average about 60 cents a minute peak.

The largest cellular telephone company is now Southern Bell

company is now Southern Bell Corp. It bought out Metromedia’s nationwide rights for \$1.65 billion. The FCC originally broke the cellular frequencies into three bands, giving one to the fixed telephone company (the wireline carrier), one to a nonwireline carrier and saved one for the future. However the distinction has become arcane as name RBOC’s (Regional Bell Operating Companies) purchase cellular rights in other cities (with our local phone revenues we subsidize their investment in real estate, manufacturing, and all sorts of things having nothing to do with our dial tone). Southeastern Bell now competes against Xerox in Boston and New York, Bell Atlantic in Philadelphia and Baltimore, Washington, and American in Chicago and Dallas. It also got about \$10,000 paying customers in sixteen cities. US West also competes against a fellow





Nasty Business

By Gene Smith
123 Main St.
New York, NY 10001
(212) 555-1234

February 5, 1987

Dear FCI Customer:

As RCA continues to grow and expand its long distance network, we have become subsidiaries to a private service all long distance companies. Toll Free - or making long distance calls on another individual's account -- is an interesting-rate problem that has been increasingly steadily.

We are concerned about toll free, and are asking you to help us. Personal Identification Number (PIN) to help prevent abuse on our customer's lines. Similar to a bank PIN code, occurrence will be returned to that their PIN code last being their authorization code.

Within the next several weeks, you will receive your Personal Identification Number and dialing instructions. We will also tell you on what date you should begin using your code.

If your telephone equipment is programmed to dial toll free numbers and authorization codes, we will have to work with you to re-program your equipment. Do not allow service interruption, please contact your Allen in our Customer Service Department, toll free, at 1-800-882-2222 by February 26, 1987. You will also be able to answer any other questions you have about this program.

Suzanna Krause
Customer Service Assistant Manager
RCA Corporation

125 SPRINT
3901 STEWART
DALLAS, TX 75247

02703786 18120663 1083 123

02/05/85 18:43:13 MDM

Attachment: 05 Sprint Customer

A review of the number of calls made on each customer code is a part of our daily relationship program. A recent review of your account shows a significant increase in calls as compared to your previous usage.

We were unable to contact you by telephone today to discuss this, and because we were concerned the calls being made on your code were unauthorized, we have suspended the code in question and will issue a new code as soon as you contact our Customer Service Department. Call us toll free at: 1-800-511-4645

We apologize for any inconvenience caused by this procedure and thank you for your continued business with us Sprint.

Sincerely,
05 Sprint

WE SEEM TO BE GETTING LETTERS LIKE THESE EVERY COUPLE OF WEEKS. SOME, LIKE SPRINT, CAN'T EVEN GET THE DATE CORRECT!

E-MAIL

CORNWALL

(continued from page 5)

also think that because there were so many videotaped services, Prestel and Type III services to look at not on the whole. British hackers weren't so much interested in big computer networks so it took them a bit longer to discover PSS and the various university networks like JANET (Joint Academic Network) and things like that.

In essence there is very little difference in the culture but a slight difference of a precaution in terms of what they are looking for.

As a system, what do you think of Prestel? You could go on and on and on about that. Prestel is extremely interesting as a matter of history. It had enormous ambitions, but its ambitions were all turned about the year 1975 which was some before anyone visualized the home computer as being possible, so Prestel visualizes and defines them. People accessing computers via their television sets. Which is why you got a 40 by 24 character display, three when various graphics which was a function of the belief that

"...this idea that the hacker can somehow fight back, that's the reason why non-hackers admire them so much."

inary was going to be an inherently expensive and that it's of display memory was really as far as you could go.

Also that the ordinary untrained person could have had to have all your comments being sale numbers. So you get this curious electronic card like type of structure and everything is available via pages or very simple numeric routing commands. Because Prestel is stuck with all of this sort of thing and if you like the man knowledge about computers moved on fast, Prestel has to become more sophisticated than a computer with the 1975 format and a lot of the things you would want to be doing on a public access database, unbelievably slowly. For example, you can order things, all the shopping and what have you, but you have to do it via a system and a gateway which is essentially, the way

it works is that the gateway opens to receive a command string from you and it closes, the command string is processed in the remote computer, the gateway opens to give you the answer and closes again so on and so forth. Any more slightly more complicated interaction is inherently slow.

You could run an online service with view data as the front end processor, but it looks ridiculous, it behaves in a ridiculous format, so the British types of services I suppose it's not too late. As the training a horse and buggy type of system where everyone is going around in gas powered internal combustion engines.

Can you see Prestel evolving down what it is now? I don't think it will do, they're trying to make it evolve but I think it is going to remain as a historic curiosity. It's fairly straightforward in one or two houses, particularly they have made it's quite useful for tax moving financial data. It will make very, very small improvements but it will be relying on its residential user base. The way people are using it now is via simulators on personal computers. On my personal computer I obviously got video text, Prestel in other words type software and it's no effort to call into Prestel or any of the other online services.

I just can't see any electronic publisher surviving. Of course although we're usually going to have to use the thing, this is wonderful in fact, most electronic publishers nowadays publish in a variety of formats, they publish in an online format, they publish in a visual text format, and of course if their material is suitable they would also be thinking about publishing in a CD ROM type format and anything else that becomes available. It's merely a format and the decision to publish and is well, are there going to be enough people out there to make it worth my while? Of course publishing in the form that you mentioned how does it work over time, everything is online?

Well, you have a variety of systems, electronic publishing for the financial community, which is obviously the most lucrative area, is still very hardware bound in that if you want to get the service then the way the supplier wants to be you have it is that you have to buy his hardware and kind of own the least line as well as getting the service.

That's the case with Reuters, they're under a lot of pressure to get rid of that and it's difficult to find other services. You can look into them because there is always extra that's always on line, that's not always available and then if you can fiddle with a personal computer system clearly, you can get the services. Other forms are basically available online and you get it via PSS which is the British Telecom equivalent to Teletext or Tyntel.

Some Suggestions

Dear 2600:

I would like to thank you for your superb magazine. It would be a big plus this year if you could: 1) Show people what to do with a blue box now, before its death; 2) Teach how to hack a code with or without a computer like in your May 1986 issue; 3) Put out a list of exchanges like 950-1088 or 950-1033 etc. with the equivalent in 800 numbers and also tell us how many digits for their access code since it appears that some of them have more digits than originally.

I observed in Manhattan some fellows dial 950-1088, enter a valid access code plus a number (with the 517, 219, 601, or 505 area code and trunk it with 2600 hertz then KP 809 XXX-XXXX ST and reach their party in Santo Domingo. I wonder whether you could explain how they avoid CCIS.

In your May 1986 issue, page 3-9B there is an algorithm by Nymex Phreak which was one of the best. It was good for one month as described, but apparently some executive at MCI read that article and in June the message was changed to confuse people but with a little ingenuity you could still hack numbers according to the same explained principle. I had kept a list of codes which I used until December 24, 1986 on which day their computer invalidated all my codes. I would greatly like to know how many digits they use in their access code. Enclosed is a self-addressed envelope so that you could provide me with a reply.

The Perpetrator

Here's your reply in a different envelope. We wish we had the time to reply personally to all of the letters we get but we simply do not.

We've published lists in the past of 950 numbers and 800 numbers as well. We'll be doing this again shortly. As far as how many digits are in a

particular company's codes, it would be a full-time job to keep track. Almost every day some long distance company somewhere changes their code pattern. Some even have more than one pattern. And quite a few have codes of varying lengths. If it's any help, our MCI codes are all five digits and our Sprint codes are nine. Beyond that it starts getting complicated.

We've printed full instructions in the past as to how blue boxes are used. They do still work perfectly from a few locations to a few locations, but they become fewer every day.

Some Numbers

Dear 2600:

Here are some phun numbers to call in the 716 area code:
888-3000 to 688-3010—University of Buffalo (MAX/CYBER!)
878-5533 and 878-4611—Buffalo State Computing Service
874-9751—Computer Science
681-8700—BOCES
886-0720—Ticketron Buffalo
836-0000, 837-0000, 850-0000, 854-0000, 855-0000, 856-0000—weird tone.

I don't understand these numbers with weird tones and suffixes of 0000—is there any explanation to this? And does this happen in other area codes? Thanks.

Silver Bandit

Yes, it happens everywhere. Those are probably test numbers from the phone company. Why don't you call one and have it show up on your local bill? Then call the phone company and demand to know who that number belongs to and why it's on your bill. That's the easiest way.

On Cellular Phones

Dear 2600:

Congratulations for beginning to publish articles on cellular telephones! The only thing wrong with the article

was the title—"a look at the future phreaking world." Cellular telephone phreaking is not in the future. To my knowledge, cellular telephone phreaking has been going on for about four years in at least one major metropolitan area. The lack of detailed information on cellular telephone phreaking in this publication has thus far placed 2600 in the dark ages.

Computer-assisted blue boxing is still essentially the same as blue boxing in the dark ages of 1961. The same MF tones were used in 1961 and the phreakers were very successful. The advantages of using cellular telephones for phreaking and hacking instead of using land lines is outstanding. Cellular phones are the most immune to tracing even if used from a fixed location and it is virtually impossible to be nailed if you use one from a different location every time and for short duration or while you are travelling on a highway.

You mentioned in the article that for detailed info, you should consult EIA Standard CIS-3-A. This publication has been outdated and has been replaced with FCC. Everyone interested in using cellular phones to their full potential should order all the publications on the subject from EIA, 2001 I Street NW, Washington, DC 20006, or you can call them at 202-457-4900.

The New Age Phreaker

We have yet to hear from a group of cellular phreakers. Though we don't doubt they exist. By the way, have the Newspapers wrong as begun saying cellular yet?

ANI Trouble

Dear 2600:

The man who asked the question in the "Letter You Wrote" page, in the November issue, signed "Frustrated in Miami" regarding his ANI. Evidently didn't read the Miami newspapers.

Some time ago, a school administrator named Johnny Jones was accused of stealing school funds. Unknown to him his telephone had been tapped.

This is an excerpt from the Miami Herald newspaper.

"Why, you may have wondered, did Johnny Jones continue to call his friend in Maryland despite the suspicion that his phone was tapped? Because, transcripts of those conversations disclose, Jones believed he had a secret number that told him whether his phone was tapped. Jones mentioned the number in almost every conversation with his friend and explained that if you call the number, your phone is clean. If you call and get a busy signal, your phone is tapped.

"Wrong. That's a lost number for telephone installers," says a Southern Bell spokesman. "When they go out, installers have to hook up a lot of wires, and that number is a final checkpoint to see if they've got the right ones connected." The spokesman says the phone company has lots of test numbers and a number for almost every one. "As for the number Jones called, if you call it and get a busy signal, it simply means the line is busy, not that your phone is tapped."

The number, incidentally, isn't located in some supersecret vault in Langley, VA. It's in an electronic switching station off Rendlesham in South Dade, OK. OK. Call 1-200-866-5763.

If you have a letter to send to us, feel free to write. Don't ramble on for too long or we'll have to chop bits out. The address to write to is 2600 Letters Editor, PO Box 99, Middle Island, NY 11953.

Error Handling

Service order transactions interact with the user frequently. Each time the transaction is ready for new input, it will respond with an underscore at the beginning of the new line. This indicates that the preceding line is correct. If an error does occur, the transaction will respond with an error message and prompt for correction. When an error occurs, you have 4 choices: 1. Re-enter the entire field correctly; 2. Enter line-lead to ignore (checks rest of line); 3. Enter a "*" to disregard the present circuit; 4. Enter a "-" to the transaction will disregard all input and exit.

H-LINE Input

H-LINE input for the service order trio SOE/CSA/ISA is being rigidly defined according to three categories. These categories contain fundamentally different types of order/facility information for the order.

Category 1: ORD, DT, DD, FUD, OC, OT, SG, EO, LC.

Category 2: US, FEA, CCF, CAT, BIN, SS, AQ, R2, FR, GP/CG, CTX/CS/MG/NNX, LDM, HTI, Category 3: PW, RW.

Category 1 items are primary—once defined they cannot be changed by conflicting category 2 and 3 lines.

Service Order Transactions

Transaction	Definition
SOE	Service Order Input
TDZ	Telephone Number Assignment lists
LQZ	Line Equipment Assignment list
SDH	Service Order Withdraw
SDM	Service Order Modification
SOE	Service Order Cancellation
SDW	Service Order Withdraw
SCM	Service Order Completion by MOF
SCP	Service Order Completion by PAO
SCA	Service Order Completion Automatic
SCF	Service Order Completion for MOF automatic
SCI	Start Cable pair inquiry
CCD	Change Due Date
BAI	Bridge Lifter Assignment Inquiry
LAI	Line Equipment Assignment Inquiry
NAI	Telephone Numbers Assignment Inquiry
TAI	The pair assignment Inquiry
EDZ	Facility Emergency Assignment list for backup

MAP Manual Assignment Parameters

MAP Manual Assignment list

TSM Total Service Order Withdraw

Transactions Defined**SOE—Service Order Establishment**

Establishes a pending service order. The types of orders are: MC, CD, OH, I, T, SS, RS, R, RF. Restrictions are treated as change orders.

H-LINES must contain OH, DD, and OT. Optional facilities: PW, PW, FUD, AQ, FA, SG, and other DT or DO.

I and O LINES may contain US, SEA, CP, OE, TN, RZ, NNX, PL, TP, TK, SL, SE, CON, MR, BTM, RC, RF, RT, STC, STN, STO, CCF, LOC, and RTI.

ESS orders requiring coordination by the recent change input carrier may be flagged with an input of "SN, C".

Example of an MC (New Connect):

```
MC BE
F 24 00000000 01-01-85 00 00 00 00 00 00
J 7 7 0001-000000 100 000 0000 00 00
```

Example of a CD (Complete Disconnect):

```
MC SE
S 28 000000 01-01-85 00 00
J 7 7 0001-000000 100 000 0000 00 00
```

Example of a CH (Change):

```
MC BE
F 24 000000 0000 01-01-85 00 00 00 00 00 00
J 7 7 0001-000000 100 000 0000 00 00
```

Example of SS (Suspension):

```
MC SE
I 175 00000000 0000 01-01-85
J 7 7 0001-000000 100 000 0000 00 00
```

TDZ—Telephone Number Assignment List

List the indicated number of separate directory numbers for a RMX code, and directory number type.

Up to 25 directory numbers can be specified, using the prefix LC.

Example:

```
LC 2 21
F 24 000000 0000 01-01-85 00 00 00 00 00 00
J 7 7 0001-000000 100 000 0000 00 00
```

(Continued on page 20)

CORNWALL

(Continued from page 11)

There are also categories that use a Pressel. Like format but are not Pressel and you can get a number of services that way as well for example the equivalent to TSM for credit checking data is called CMM. That's available in the user's local format. That doesn't come out via postal, it comes out via its own data network and there are other data networks with other services on them as well. So that's basically how it works.

Have you planned any future books on computer crime?

Well, I am writing a much more serious book at the moment called "Data Theft" which is intended for the chief executive officer of the CDD market and that is encouraging those people to believe that they can't leave data security to a mere technical subsidiary. Through it is much more preoccupied with industrial espionage and fraud. It is not going to be in any way a unique and cheap book. That of the "The Hacker" was alleged to be a book on computer security, but is marketed for hackers. This is a book on computer security and it is intended for chief executive officers and I don't think hackers would find it of any direct interest though I hope they are going to read it.

One of the things I'd want to get over is the notion that most computer crime is controlled by insiders, computer criminals are normally employed by their victims. I want to talk about police hunting or rather the lack of it, the lack of responsive criminal procedure with it. I will say that there is a bit of room for talking about technology and I really like to promote looking for what I believe is its rightful place—something for a try, try money to finance themselves with without actually causing any serious harm to anybody.

In the book "The Rise of the Computer Star" the author put forward the premise that new technologies require computer bureaucracy and thereby also build up a very well developed, everything, and every year could you see hackers as a possible disease?

I have been asked this question in a slightly different form before. Not really, I think the root of computer crime, although these files can be built up, the files themselves are not necessarily entirely reliable. One of the great problems with interactive data is that they collect together so much information and so much gossip that although they can have it all on the screen in front of them they don't know whether it's somewhat dubious or not at all. One of the reasons why I think there is so much room in people's brains for the hacker is that they believe the hacker is going to provide that sort of defense which you were describing. I actually wrote a piece for one of the papers about it about folk being sitting for example King Arthur's a very potent figure, Robin Hood's a very potent figure, and the galaxy of these things is that King Arthur is going to be [the] one and future King, Robin

Had you known not a great deal about King Arthur, Robin Hood but the great thing was that he stole from the rich to give to the poor and that probably is why he is remembered.

I think it is this idea that the hacker can save you right back, that's the reason why non-hackers assume men so much. I am afraid I don't believe that hackers are sufficiently good or sufficiently powerful or sufficiently able to control that. I do think that every now and then though what a hacker can do is it is very busy, expose the stupidity [of] some of the power that is held on computers and maybe just enough that there is that element of defense that you're looking for. But on the whole I would say the outlook for people/individuals in the near future age is not very good.

The Hacker's Handbook

By Hugo Cornwall

E. Arthur Rowe Company, Alexandria, VA

169 pages

\$12.95

Review by Roland Dutton

Strangely enough, this book actually lives up to its title. The author's stated purpose is to help the reader grasp the nomenclature and develop the appropriate attitudes and skills, provide essential background and some reference material, and point you in the right direction for more knowledge. In this he succeeds, and in the meantime he gives us a lively and entertaining view of the world of British hacking.

The early chapters of the Handbook discuss the technical details of computer communications, the physical hacker's equipment, and the types of services or "targets" that a hacker might be interested in. The technical explanations are clear and accurate, and are neither too difficult for the beginner nor so simple that the seasoned system cracker might not learn a few details from them. In general, the entire book appears to be an excellent beginner's manual, a very good intermediate manual, and enjoyable though certainly not indispensable reading for those who style themselves "hackers".

Two more chapters discuss "hacker's intelligence" and "hacker's techniques". Then computer networks and viruses are discussed. The index (also known as "vindex" or "vindexer") chapter is interesting for American readers since none of those types of services are available here, and it's always interesting to know what's

telecom informer

(Continued from page 8)

RROC, Pacific in San Diego.

800 number allocation

It used to be that you could tell the geographical location of an 800-NXX number by the NXX part. XX2s were interstate, XX3s were in Canada, and every prefix represented an area code. However, about five years ago AT&T introduced "Advanced 800 Service"

which permitted any INWATS (Inward Wide Area Telephone Service) call to be routed anywhere in the U.S. and even to different destinations depending on both the time of day and where the caller placed the call. (Thus 800-DIAL ITT would reach the nearest ITT billing

complaint center during the day, and at night the call could instead reach a main office left open. The company has to pay for the normal 800 INWATS lines and then an extra couple of hundred a month for the "vanity" number and a few cents for each translation of end phone line by time or location.

Until Fall 1986 if your CO was switched over to equal access your 800 call was routed to AT&T so either what your default carrier. But now your CO must route all 800 calls to MCT

which have any of these "exchanges": 234, 283, 284, 288, 289, 274, 333, 365, 444, 456, 627, 666, 678, 727, 799, 777, 825, 876, 888, 937, 950, 958, and 999. US Sprint gets 728 and WLD Metrolane gets those to 988. The individual BOCs get the XX2 exchanges (as these are filled with interstate WATS lines). More exchanges will undoubtedly be grabbed by other carriers as they begin to offer 800 service. I don't know what happens if your company's 800 number's exchange gets taken over by Bargain

Bob's Telephone Company. Hopefully you get to keep the old provider, but this would really make it tough to route. Don't know what happens either if your clever little phone number "vandy" belongs to Bargain Bob, guess you gotta suffer. If your CO isn't equal accessible yet, it just kicks the call onto the nearest

intra-ATA tandem site for the proper routing.

However, don't bother to remember this. When Bellcore finally finishes the new Advanced 800 service the INWATS buyer can route his or her incoming call through a different carrier depending on the originating point or the time of call, as well as sending it to a different

company office. When this happens all 800 calls will have to be sent to the nearest tandem switch and get routed based on all this info. The final info will get the money for providing the routing service.

As far as I know only AT&T gets your 900 calls, which were never

grouped according to geography. Trivia fact number 1: INWATS numbers in England (to the US, International INWATS) further confuses the geographical delimitation) are of the form 0800-XX-XX-XX. Only AT&T provides this. Trivia fact 2: INWATS was not introduced in 1967 as stated in the December 26/66, page 3-95. The first interstate INWATS lines were in 1967, but interstate INWATS started in 1966.

Airfone Update

The future of Airfone, the pay telephone for use on airline flights is in limbo. Airfone's experimental license expires at the end of 1987, and the FCC will not reconsider its January 1985 decision refusing permanent frequencies. Airfone expects to continue with over 3000 plane phones and the 65 ground stations even though there is no provision for frequency allocation. Airfone hopes to be allowed to use cellular frequencies.

More Nasty Business

```

          0000000000000000000000000000000000000
          0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
          0000000000000000000000000000000000000
    
```

ADMINISTRATIVE MESSAGE

ROUTINE

F 071515Z SEP 86 278

FM CNO WASHINGTON DC

TO NAVOP

BT

UNCLAS//FORN//

0000 000/00
 50007 TELEPHONE CREDIT CARD FRAUD

1. TELEPHONE CREDIT CARD FRAUD CONTINUES TO AFFECT PEOPLE REGARDLESS OF JURISDICTIONS BY COMMANDS AND THE HELP OF THE ABOVE INVESTIGATIVE SERVICE.

2. CONTRACT TO PERSONS BELIEF, THERE IS AN FEEL LIKE STRANGE TELEPHONE SERVICE FOR OUR PEOPLE TO CALL ANYWHERE IN THE CONTINENTAL UNITED STATES OR OVERSEAS. HAVE PEOPLE BEING USUNNORMALLY CREDIT CARD OWNERS ARE BEING CALLED FROM CONSPIRACIOUS CARRIERS AND BEINGING STRATEGIT TO THEMSELVES AND THE WAY. STATUS OF TELEPHONE CREDIT CARD, MONITOR OR FRAUDULENT USE OF APPROPRIATION CODE NUMBER WILL NOT BE TOLERATED. VIOLATORS ARE SUBJECT TO CRIMINAL PROSECUTION UNDER THE FCMA AND CIVIL STRONGER, AS WELL AS ADMINISTRATIVE ACTION.

3. AN APPROPRIATE NUMBER OF EDUCATION, APPREHENSIONS AND POINTMENT IS NEEDED TO STOP THE TROE.

BT

CFM 0307/230

0208

91 0317 139/19-872

071232Z SEP 86
 CNO WASHINGTON DC

```

          0000000000000000000000000000000000000
          0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
          0000000000000000000000000000000000000
    
```

**Remember
the Greediest!**

NEW DEVELOPMENTS

They've done it again. Our phone company has figured out a way to make a punch out of absolutely nothing. While we must commend them for their ever-present ingenuity, we must also point out that this is indeed the way best to screw.

We all know how unjustified the charge for touch-tone service is. Touch tones make phone company equipment operate a lot faster, yet people can be fooled into thinking they're getting "access" to some kind of premium service. But the fact is that we all have access in the first place and the only way the phone company can charge this is to invent a machine that makes your touch tones useless if you haven't paid. That's why touch tones work regardless of whether or not you pay for them on older phone systems. They're not sophisticated enough to operate that horrible machine. Remember—you're not actually paying for the service—you're paying for not being disconnected from the service.

The newest ripoff is a feature called "gold numbers." Do you remember the days when you could get a phone installed and ask if you could get a particular number? If the number was available, you'd be able to get it in most cases. Just like that. Well, you can kiss those days goodbye.

"For less than a quarter a day," the cheery little New York Telephone pamphlet says, "you could have a number that is easy to remember because of repeating or sequential digits. Or you might select any available 7-digit combination of numbers in such your needs, perhaps trying for a number that translates into a word or phrase."

Isn't this brilliant? As if nobody had ever thought of selecting their own phone number before! And, since they were smart enough to come up with the idea, they've naturally earned the right to charge us \$3 a month for one of these numbers or \$6 a month for business customers. Maintenance charges, no

doubt.

That's not enough! OK, here's some more. If the first three numbers you ask for aren't available (which doesn't necessarily mean they're being used), guess what happens? "A fee of \$20 will apply for each 3-number search beyond the initial one." Twenty dollars just to apply for a number! And that's no guarantee you'll even get it! It could go on forever!

Obviously, the phone company is going to clean up on this if people are foolish enough to fall for it. One night after the other, we're seeing services that have always been free develop charges. While some changes in services are necessary because of the diversion, this is certainly not one of them. It's time some nasty letters were written to our elected officials who have the power to do something about it.

Gold numbers, indeed. Would anyone care to speculate on what they're going to try next? Meanwhile, there's an entirely new service that has sprung into being overnight. It's called PRS and it's being used by Mountain Bell and Pacific Bell. PRS stands for Personal Response System and means exactly the opposite. It seems that when you call up a directory assistance operator in those

regions, the voice you hear saying, "Can I help you?" or "What city, please?" is actually a recording! Each operator records their own "greeting" and it plays when they pick up. This, according to the company, gives the operator some time to rest between calls. In fact, they like to refer to it as "the Pause that Refreshes and Satisfies." They say the customers just love it because the recording sounds so friendly and upbeat. Give us a break! It's just another way of turning those poor operators into machines. There's already a recording that gives the number, now there's one that picks up the phone! What's left?

2600 marketplace

DOCUMENTATION on electronic & digital FAX's and switching systems. Willing to trade/purchase. Also looking for Bell System Practices and other such paraphernalia. Write to Bill, c/o 2600, PO Box 7628, Middle Island, NY 11953.

CELLULAR TELEPHONE INFORMATION WANTED. I will pay a modest fee for info which has not yet been published in 2600. Please describe the type of info that you have and name your price. Mr. S., P.O. Box 2895, Brooklyn, NY 11202.

MANUALS OR INSTRUCTIONS NEEDED for two modems labeled Dataphone Channel Interface. One has label on the outside that says: 40A2 Series 1, Data Mounting, SD-1D247-01-J23 and the other says: 44A2 DATA MTG. SD-1D247-01-J23. SERIES 1 83 MG 12. The boards on the inside are labeled DAS 8298-11A, SERIES 4, 81MG3 and DAS 8298-11A, SERIES 5, 84 MG 04. Send info to: P.O. Box 60346, Raleigh, NC 27650.

PRIVATE INVESTIGATOR wants to hear from 2600 readers who have electronic equipment he can buy cheap! Gaslamp Private Eye is into Electronic Counter-measures/TSCM in the marketplace. 425 "F" Street, San Diego, CA 92101, (619) 239-6991.

TAP BACK ISSUES complete collection, vol. 1-83 plus supplemental reports and schematics. Approx. 400 pages of quality copies sent via UPS or US Mail \$100 includes delivery. Send cash, check or MO (payable to PELL). Cash sent same-day, others allow 4 weeks, to: Pete G., Post Office Box 463, Mt Laurel, NJ 08054.

HEY YOU! This is the chance you've been waiting for! A new service of 2600 Magazine. Got something to sell? Looking for something to buy? Or trade? This is the place! And it's free to subscribers! Just send us whatever you want to sell (without making it too long) and we'll print it! And, if you send in the only ad we get, you'll get the entire page to your self! Only people please, no businesses!

Deadline for March issue: 3/1/87.

Duplicate example would look similar to this:

```

HEADLINE FACILITY (EXAMPLE) 157 11-21-83
SERVED LINE EXAMPLE
NOI SERVED LINE EXAMPLE LINE
MACHINE ADDRESS (SERVED TO)
244-1010
244-1010, etc.
NOI ADDRESS (SERVED TO)

```

SOW—Service Order Withdrawal:

Withdraws most recent version of a service order.
 • Order number must refer to the latest version.
 The H-LINE circuit ID identifies the order. Valid circuit identifiers are: TN, KM, PL, CP, OE, and TX.

Example:

```

MG 534
P 100 100 100 100 100 100 100

```

SOP—Service Order Completion by PAO:

Records in the Service Order File the completion of an order by PAO.
 • Standard SXX H line input

Example:

```

101 100 100 100 100 100 100

```

SQA—Service Order Completion Automatic:

Files final completion on all service orders which have been or are not required to be completed by the PAO, and not in a held or leopardy status, and are due prior to or on the current date.

• Two due dates may be entered on the H-LINE. SCA will complete orders due on or between the dates. Additional orders are OT (order type), ORD, and SG.

Example:

```

MG 534

```

(complete all orders on or before this due date)

Example 2:

```

MG 534
P 100 100 100 100 100 100

```

(complete all MG lines correct orders)

COO—Change Due Date:

Change due date of a service or name order.
Example:

```

MG 100
P 100 100 100 100 100 100

```

Output Example:

```

MG 100 100 100 100 100 100

```

KM—Telephone Number Assignment Inquiry:

Provides from 1 to 25 your telephone numbers compatible with the input specifications.

• Input is an H-LINE with the TN type and RMX or RZ entries. The status of the TN supplied will be modified to reserved if S1 is specified on the H-LINE.

Example:

```

MG 101
P 100 100 100 100 100

```

(This shows first available space in prefix S34.)

MAP—Manual Assignment Parameter:

Permits the PAO to establish the parameters that will constitute the PAO Report-of-Day report.

Example:

```

MG 102
P 100 100 100 100 100

```

(for telephone numbers of type B, 101)

(Thanks to Tom, Don Eps, and Sir Galahad for their contributions.)

In the future we will be devoting more time to just what COSMOS means to the average person and how it can effect and disrupt their lives. There are many other computer systems that are capable of doing all kinds of other things to your personal lives. We welcome information and comments on them all.

Write to 2600, PO Box 99, Middle Island, NY 11953-0099. Or call the office at (516) 751-2600.

Reviews

(Continued from page 15)

going on elsewhere. As one might expect from a British author, the discussion of computer networks centers around the British public data networks, which are similar to Telenet or Tymnet.

And for those hackers who have too many security officers chasing after them, one chapter discusses "radio computer clubs", also known as radio teletype or RTTY. This is not really hacking, but just an interesting way to use your computer when you're not moving satellites with tank parts ordered from TRW. You need a short wave receiver and an interface (which starts at \$40), and you will be able to tune in various stations that use the international short-wave bands for transferring computer data. Sample listings in the book show a news bulletin about the Enver Hoxha Automobile and Tractor Combine in Albania, and some typical amateur radio conversations.

Every chapter always has one or two lines or techniques that the capable hacker can use to expand his or her horizons. Here's one fun idea that rarely gets discussed, under the heading of "Handmade Trucks":

"For the hacker with some knowledge of computer hardware and general electronics, and who is prepared to mess about with circuit diagrams, a soldering iron and perhaps a voltmeter, logic probe, or oscilloscope, still further possibilities open up.

"One of the most useful bits of kit consists of a small, cheap radio receiver (RMW/JAM brand), a microphone, and a tape recorder. Radio in the vicinity of computers, modems, and telephone lines can readily pick up the drip drip of digital communications without the fuss of carrying out a physical phone tap. Alternatively, an inductive loop with a small low-gain amplifier in the vicinity of a telephone or line will give you a recording you can analyze later at your leisure."

[An inductive loop is a long piece of wire wrapped

around in circles placed next to the line that you want to listen to. A typical inductive loop is the section cup microphone that sticks to a telephone handset and records the conversation without being physically attached to the line.]

Overall, *The Hacker's Handbook* is a good book for those hackers who want to broaden their horizons, or who just need some new ideas. Hackers on both sides of the pond will get a better understanding of the regular machinery that places all this thrillingating telecommunications within our grasp.

Automatic Teller Machines III
 by John J. Williams, MSEE
 Cosmometrics Co.
 P.O. Drawer 537
 Alamygordo, NM 88310
 \$25.00

Review by Lord Phineas:
 Automatic Teller Machines (ATMs) are the wave of the future in banking. Projections aimed at 500,000 ATMs and Point of Sale Terminals (POS) in place by the year 2000. By 1990 there will be \$550 billion worth of ATM transactions per year. ATMs are becoming a major force in the banking industry, with more than 88 million Americans using them. But along with the added convenience and lower costs to banks of using ATMs, crimes involving these machines have grown enormously as ATM use expands.

Reported ATM crime in 1983 was between \$70 and \$100 million, and estimates run as high as \$1 billion. These figures don't include nudgings and other crimes directly against ATM users. With \$50,000 in a newly refilled ATM, "a veritable cookie jar," these machines are becoming the focus of criminals. ATM fraud soon will become a major criminal activity.

John Williams begins his pamphlet with a series of apocalyptic warnings about the repercussions of this boom in ATM fraud. According to his "Background Information", John Williams is very convinced of the danger this growing area of fraud poses to the American public. His apocalyptic visions get carried to extremes, as he states that "I strongly feel that all forms of EFT [Electronic Funds Transfer, which include ATMs] are instruments of Satan



and must be developed to prevent or slow down by the "Artificial." These five forebodings are interspersed throughout the text, complete with references to Big Brother. Williams also dislikes the banks and other capitalist enterprises. He claims it is in the banks' best interests to suppress stories of ATM fraud losses. ATM transaction costs are much less than those dealing with live human beings. In addition, Williams claims that once banks have gotten the public to prefer using ATMs, they will raise charges to the customer for ATM transactions. He also warns against the "ominous risks to our freedom and privacy as the ATM invades the home." Although these claims certainly make entertaining reading, they detract from the seriousness of the work and make it too easy to dismiss. However, once one gets beyond these ravings one realizes that there actually is some useful information here.

One area where the book excels is the section dealing with preventing oneself from fraud. Many of the suggestions are common sense, but many people don't even think of using them. Williams is especially concerned about violent crimes against ATM users by robbers. For example, he suggests that one never withdraw funds between 10 and midnight, as criminals can then make two days of maximum withdrawal with your card. Williams also addresses your legal rights. If a violent crime occurs within the ATM lobby, you can probably successfully sue the bank for improper safety measures. The section on how many ATM scans work is helpful, as most of them involve some form of tricking the victim into revealing his PIN. He also lists several warning signs of ATM fraud in progress or about to happen so one can avoid becoming another victim. The section on protecting oneself from fraud perpetrated by bank employees as well as more common criminals is indeed valuable, as is the discussion on EFT laws.

The technical section is interesting, but not very useful. Williams focuses on the old-school ATM, which accounts for about 45% of installed ATMs, but one wonders if the information is out of date or only applies to one model. There is a discussion of several other models as well. He does, either in a useful and interesting explanation of ATM card magnetic strip formats,

as well as encryption schemes. This really is the most interesting and informative part of the entire booklet, as he in depth discusses PIN encryption and data formats. The technical sections on how ATMs and ATM networks operate is also interesting, although not specific enough.

If you bought the book with the hope of finding out an easy way to break into an ATM machine, forget it. Most of the methods are sufficiently vague that you would have to do much more investigation on the topic anyway (luckily for the rest of us). Many of the physical attack methods are just the same as for pay phones (or any other armored object, though surprisingly many ATMs are only fire resistant, not burglar or bomb resistant), and are rarely really obvious. Many of the successful methods used in the past are due to programming mistakes which probably have been repaired. ATM security seems to be rapidly evolving. Bad and major holes are patched as soon as they become apparent. The section on computer related break-in methods was especially vague, and much of the material was too generalized and could be applied to any computer crime.

When one comes to the end of the booklet one wonders if it was worth the cost. Twenty-five dollars is a lot for 118 pages (plus a three page feedback questionnaire) of barely vetted ravings. Each page, however, is two columns of very small print, containing some information of worth, most of which is impossible to find from any other source. The diagrams aren't particularly helpful, mainly being cartoons and publicly shots. Williams often plugs his other books in the work, as well as America's Privacy Radio, which is defuncting (admittedly, he also plugs 2600 as "the best source on phone and computer phreaking"). This moved a better investment if the ravings were removed along with a lot of the extraneous material. It isn't especially useful to scan through columns of clippings falling that so-and-so stole such-and-such amount somewhere. Many of the clippings really have nothing to do with ATM fraud, and are merely filler. My suggestion to the author for Automatic Teller Machines IV is to cut out much of the clutter, which detracts from the seriousness of the topic.

ATTENTION

These are the new prices now in effect. You can still save money and hassles by renewing for two or three years.

- \$15 1 year subscription or renewal
- \$28 2 year subscription or renewal
- \$45 3 year subscription or renewal
- \$40 1 year corporate subscription or renewal
- \$75 2 year corporate subscription or renewal
- \$110 3 year corporate subscription or renewal
- \$25 overseas subscription or renewal (1 year only)
- \$55 overseas corporate subscription or renewal (1 year only)
- \$260 lifetime subscription

Back issues have new prices too. They are:

- \$25 1984, 1985, or 1986 issues (12 per year)
 - \$50 Any two years
 - \$75 All three years (36 issues)
- (Overseas orders add \$5 for each year ordered)

Send all orders to:
 2600
 PO Box 752
 Middle Island, NY 11953 U.S.A.
 (516) 751-2600